NewsNet

National Cybersecurity Strategy

The President's Critical Infrastructure Protection Board has issued a draft of the National Strategy to Secure Cyberspace that calls for extensive participation from both the public and the private sectors. The board emphasizes that the document (www.whitehouse.gov/pcipb/draft) is a work in progress and the final plan will depend heavily on feedback from the public.

The strategy, which is described in its introduction as "not written in stone," categorizes concerns into five levels: the home user, the large enterprise, critical sectors, the nation and the global community. Other core components include cyberspace threats and vulnerabilities as well as policies and principles that will guide the strategy.

Some of the recommendations for the home user involve basic safe computing practices such as installing firewalls and maintaining up-to-date antivirus software. Internet service providers, security firms and software designers should collaborate to improve security development and implementation. Large enterprises should form both internal and external boards or organizations to coordinate security efforts. These might include public-private partnerships to determine best practices.

Critical sectors of the federal government must, by the fourth quarter of fiscal year 2003, complete a comprehensive program performance review of the National Information Assurance Program. This will follow other efforts at assessing requirements and options. The strategy also calls for the federal government to lead in the adoption of secure network protocols. State and local governments are urged to establish security programs and participate in information sharing and analysis centers.

Addressing national priorities should involve public-private partnerships that range from federal funding for information security research and development to the creation of a clearinghouse for security patch solutions. Other private-public efforts could include information sharing, training and education, certification and awareness.

All comments on the strategy must be submitted by November 18 to feedback@cybersecurity.gov.

Geospatial Standards

The National Imagery and Mapping Agency (www.nima.mil) has established the National Center for Geospatial Intelligence Standards. This effort is part of an agency thrust toward implementing a comprehensive, enterprisewide standards management policy for the National System for Geospatial Intelligence.

The National Center for Geospatial Intelligence Standards (NCGIS) will focus on standards issues for enabling technologies, data architecture and software tools. The goal is to ensure interoperability for geospatial intelligence among traditional military and intelligence customers as well as international coalition members, the private sector and elements that constitute the national system.

Teri Dempsey, chief geospatial intelligence standards officer, will lead the new organization.

PKI Bridges the Gap

The Federal Bridge Certification Authority, also known as the Federal Bridge, has cross-certified the public key infrastructures of the U.S. Defense Department, U.S. Treasury Department, U.S. Agriculture Department's National Finance Center and NASA, allowing these organizations to trust and validate the digital signatures when sharing files.

Public key infrastructure (PKI) certificates can be used to affix a user's unique digital signature to electronic documents, forms and other digital files. It offers authentication, transaction integrity, nonrepudiation and confidentiality.

According to Judith Spencer, chair of the Federal PKI Steering Committee, the committee is working with other agencies, states, governments of allies and Federal Bridge authorities to effect interoperability through cross-certification.

Mark Forman, associate director for information technology and e-government, General Services Administration, says the Federal Bridge will facilitate the unification of islands of automation across the government, potentially integrating federal systems.

Additional information on Federal Bridge is available at www.cio. gov/fpkisc.

Focus on Transformation

The U.S. Defense Department has created a new office devoted to changing the communications architecture within the national security space program. Known as the Transformational Communications Office, the new joint organization will coordinate, synchronize and direct the implementation of a transformational communications architecture.

The primary goal of the group will be to ensure communications compatibility across the Department of Defense, the intelligence community and NASA. A recent study suggests that establishing a compatible communications system using both laser and radio frequency technologies could increase capabilities by a factor of 10, but the existing baseline program plan would not meet the forecast requirements. The new office is developing a detailed architecture and acquisition strategy to achieve this goal and will coordinate acquisition and implementation of various system elements with existing program offices using established authorities and budgets.

Rear Adm. Rand Fisher, USN, director of communications at the National Reconnaissance Office and commander of the Navy's Space and Naval Warfare Systems Command Space Field Activity, is the director of the Transformational Communications Office. Christine Anderson, director of the Military Satellite Communications Program Office at the U.S. Air Force Space and Missile Center, is the deputy director.

All for One

Three pioneers in digital video broadcast-return channel via satellite (DVB-RCS) technology have submitted a joint plan to the European Space Agency that would accelerate the interoperability of the technology. Through the plan, each company would validate the interoperability of its terminal with the other two firms' DVB-RCS hubs. An independent service provider will test and certify results.

The plan represents the first active cooperation between EMS Satellite Networks (www.emssatnet.com), Nera Broadband Satellite AS (www.nera.no) and the Newtec group (www.newtec. be) to support a DVB-RCS open standard. Until the technology was introduced, satellite communications and very small aperture terminal customers had to make significant commitments to proprietary systems for two-way broadband access via satellite. Interoperability will give customers the choice of purchasing satellite interactive terminals from one or several vendors.

The plan is part of the European Space Agency's SatLabs initiative, which focuses on establishing the DVB-RCS open standard in the satellite communications market worldwide.

F-22 Simulators Gain Muscle

The U.S. Air Force has purchased high-power graphics systems for its F-22 full-mission and weapons tactics simulators. The computers are designed to give the simulators the ability to provide pilots with a realistic, high fidelity, virtual training environment.

The F-22 full-mission trainers will simulate a variety of air- and ground-based threats and environmental conditions such as wind shear, turbulence, storm cells and lighting. Two Silicon Graphics Incorporated (www.sgi.com) 32-processor SGI Onyx 3800 visualization systems with eight graphics pipes each help to create 360-degree out-of-window views, cockpit displays and simulated aircraft behavior.

Six additional 16-processor SGI Onyx 3800 visualization systems will power the Air Force's F-22 weapons tactics trainers. Each system contains a single graphics pipe to create and support a virtual tactical environment. The trainers will provide pilots with simulated controls, displays and the ability to practice using individual and team weapon systems. No training version of the F-22 is being built, so pilots must rely exclusively on simulation to train for the aircraft.

Self-Targeting Missile Cleared

The U.S. Navy has approved a missile with automatic target acquisition capability as ready for service. The weapon will provide the Navy with long-range, precision strike options against ground-based vehicles and facilities as well as ships at sea.

The standoff land attack missile-expanded response automatic target acquisition (SLAM-ER ATA) capacity was declared operationally effective and suitable by the service in September. It is the only weapon of its type with an operational automatic target acquisition capability, Navy officials say. The missile also can navigate using global positioning system data or be manually directed to a target from the launch aircraft.

A second mission computer was added to the SLAM-ER missile to provide an ATA capability. The computer's software examines data from the missile's infrared imager for target locations, permitting the ATA system to locate small targets on a cluttered battlefield and either cue the pilot or guide the missile autonomously to the objective. Additional tests are underway to measure the ability to process in-flight target updates for hitting mobile targets.

The SLAM-ER ATA is manufactured by the Boeing Company (www.boeing.com).

Security Is a Bull Market

The U.S. market for homeland security technology products and services is valued at more than $98 billion, according to a report compiled by Provizio Incorporated (www.provizio.com), a business intelligence-gathering firm. The study indicates that local government requirements constitute a $9.5 billion market and recommends specific strategies to overcome the challenges of this market.

The report, titled “Homeland Technology Opportunities: The Market, the Needs and Recommendations,” addresses the industry and the companies within it with specific references to companies that are uniquely positioned to meet local, state and national homeland security needs.

An electronic version of the report is available at www.securitysummits. com/reports.